

Multiplication matrices and ideals of projective dimension zero

Samuel Lundqvist

Abstract

We introduce the concept of multiplication matrices for ideals of projective dimension zero. We discuss various applications and in particular, we give a new algorithm to compute the variety of an ideal of projective dimension zero.

1 Introduction

Eigenvalue methods to compute the variety of an affine zero-dimensional ideal has become an active area of research [5, 6, 16, 17]. Recall that an ideal is defined to be of dimension zero when the corresponding variety is finite. The eigenvalue methods use both algebraic and numerical algorithms and the key is a nice one-to-one correspondence between the points on the variety and the eigenvectors to so called multiplication matrices.

The notion of zero-dimensionality has a meaning also in projective space. Over an infinite field, an ideal of projective dimension zero is an ideal whose variety consists of a finite number of projective points. Below we will give a general definition, valid also for finite fields. We show that it is possible to define multiplication matrices with respect to ideals of projective dimension zero. Our main result is that the one-to-one correspondence mentioned above also holds in the projective setting, giving a new method to compute the variety of an ideal of projective dimension zero.

In order to define the projective multiplication matrices, we need to choose appropriate vector space bases for the graded pieces of the quotient ring S/I , where S is a polynomial ring over some field and I is an ideal of projective dimension zero.

The usual choice of a vector space basis is the set of residues to the complement of the initial ideal of I (with respect to some monomial order). Our choice of bases differs from the usual ones — in general we consider non-monomial \mathbb{k} -bases. This choice of bases happen to give a fast normal form algorithm for high degree elements, which outperforms the usual reduction method based on Gröbner bases.

Moreover, we discuss how our approach can be used to compute vanishing ideals of projective points. We give an alternative version of the graded Buchberger-Möller algorithm and give a fast algorithm for computing projective separators.

2 Notation and preliminaries

Throughout the paper, let \mathbb{k} be a field and let $S = \mathbb{k}[x_0, \dots, x_n]$ denote the polynomial ring in $n + 1$ variables. Recall that the Hilbert series of a graded ring $R = R_0 \oplus R_1 \oplus R_2 \oplus \dots$ is the power series $\text{Hs}(R, t) = \dim_{\mathbb{k}}(R_0) + \dim_{\mathbb{k}}(R_1)t + \dim_{\mathbb{k}}(R_2)t^2 + \dots$. An ideal I is of projective dimension zero exactly when $R = S/I$ is graded and satisfies $\dim_{\mathbb{k}}(R_i) = m$ for some $m > 0$ and for all i sufficiently large. The least i such that $\dim_{\mathbb{k}}(R_i) = \dim_{\mathbb{k}}(R_{i+1}) = \dots$ is called the *postulation number* and is denoted by $\text{post}(R)$. We say that R postulates in degree $\text{post}(R)$.

When I is an ideal of projective dimension zero and $R = S/I$, we say that R is a ring of projective dimension zero. For an element a of S , we write $[a]$ to denote the equivalence class in R containing a .

By $\overline{V(I)}$, we denote the variety of I with respect to the algebraic closure $\overline{\mathbb{k}}$ of \mathbb{k} , so $|V(I)| \leq |\overline{V(I)}|$. The number of projective points in $\overline{V(I)}$ counting multiplicity equals $\dim_{\mathbb{k}}(R_{\text{post}(R)})$.

Let $I = Q_1 \cap \dots \cap Q_s$ be a minimal primary decomposition of I . Let $P_i = \sqrt{Q_i}$. When no P_i equals the unique graded maximal ideal $\mathfrak{m} = (x_0, \dots, x_n)$ of S , we say that I is unmixed. When I is unmixed, the Hilbert series of R is strictly increasing until it reaches degree $\text{post}(R)$.

When I is mixed, we will write the primary decomposition as $I = Q_1 \cap \dots \cap Q_s \cap Q_{s+1}$ and assume that $\mathfrak{m} = \sqrt{Q_{s+1}}$. The Hilbert series of R when I is mixed does not behave nice in general (it can have an arbitrary number of valleys for instance).

We need a notation to drop the primary component Q_{s+1} in the case when I is mixed, so we define $I^u = Q_1 \cap \dots \cap Q_s$. This means that when I is unmixed, we have the identity $I = I^u$. We extend this definition so that $R^u = S/I^u$.

Example 2.1. Let $I = x_1x_2^3 - x_2^4, x_1^3x_2^2 - x_2^5$. Then $I = (x_1 - x_2) \cap (x_2^2) \cap (x_1^3, x_2^3)$. Thus, $Q_1 = (x_1 - x_2)$, $Q_2 = (x_2^2)$ and $Q_3 = (x_1^3, x_2^3)$. We have $P_1 = \sqrt{Q_1} = Q_1$, so $V(P_1) = \{(1 : 1)\}$ and $P_2 = \sqrt{Q_2} = (x_2)$ so $V(P_2) = \{(1 : 0)\}$. Finally $\mathfrak{m} = \sqrt{Q_3}$. Thus, $I^u = (x_1 - x_2) \cap (x_2^2) = (x_1x_2^2 - x_2^3)$. We have $\text{Hs}(R^u, t) = 1 + 2t + 3t^2 + 3t^3 + \dots$, while $\text{Hs}(R, t) = 1 + 2t + 3t^2 + 4t^3 + 4t^4 + 3t^5 + 3t^6 + \dots$, so $\text{post}(R^u) = 2$ and $\text{post}(R) = 5$ (It does not in general hold though that $\text{post}(R^u) \leq \text{post}(R)$.) The point $(1 : 1)$ has multiplicity one, while the point $(1 : 0)$ has multiplicity two (it follows from the fact that (x_2^2) has a chain of primary ideals of length two).

We have a one-to-one correspondence of prime ideals P_i generated in degree one and points on $V(I)$. If $\overline{V(I)} = V(I)$, it follows that $|V(I)| = s$ and that P_1, \dots, P_s are all generated in degree one.

The concept of non-zero divisors is of particular importance in this paper. Recall that l is a non-zero divisor on the S -module M if $lm = 0$ implies that $l \neq 0$. In Example 2.1, $[x_1]$ is a non-zero divisor on R^u , while $[x_2]$ is not. The existence of non-zero divisors is connected to Cohen-Macaulayness and also to the primary decomposition in the following sense for a ring $R = S/I$ of projective dimension zero.

I is unmixed $\Leftrightarrow R$ is Cohen-Macaulay $\Leftrightarrow R$ contains a non-zero divisor

Although R lacks non-zero divisors when I is mixed, we will show that there exists a minimal degree d so that $R_d^u \oplus R_{d+1}^u \oplus \dots$ and $R_d \oplus R_{d+1} \oplus \dots$ are

isomorphic as S -modules. This degree d will equal $\max(\text{post}(R), \text{post}(R^u))$. To simplify notation, we will denote $\max(\text{post}(R), \text{post}(R^u))$ by $\text{nz}(R)$. When the context is clear, we will omit R and only write nz . It follows that every non-zero divisor on R^u is also a non-zero divisor on $R_{\text{nz}} \oplus R_{\text{nz}+1} \oplus \cdots$. In Example 2.1, $\text{nz}(R) = 5$ and $[x_1]$ is a non-zero divisor on $R_5 \oplus R_6 \oplus \cdots$.

Suppose that V and W are two \mathbb{k} -spaces of dimension m and m' respectively. Let e_1, \dots, e_m and $f_1, \dots, f_{m'}$ be \mathbb{k} -bases of V and W , respectively. Let ϕ be a \mathbb{k} -linear map from V to W and let A_ϕ be the $m \times m'$ matrix, whose i 'th row is the coefficient vector $(c_1, \dots, c_{m'})$ and where $\phi(e_i) = c_1 f_1 + \cdots + c_{m'} f_{m'}$. Notice that A_ϕ is the transpose of the standard matrix representation of ϕ .

When the map ϕ is defined on an a finite dimensional algebra by $v \mapsto fv$ for an element f in the algebra, then the matrix A_ϕ is called the *multiplication matrix* with respect to f . We also denote A_ϕ by A_f .

Example 2.2. Let $I = (x_1 - 1, x_2^2 - x_2) \subset \mathbf{Q}[x_1, x_2]$. The ring $\mathbf{Q}[x_1, x_2]/I$ is of affine dimension zero and a vector space basis for the quotient ring can be chosen as $[1], [x_2]$. In this algebra we have $[x_1][1] = [1], [x_1][x_2] = [x_2], [x_2][1] = [x_2]$ and $[x_2][x_2] = [x_2]$, so the multiplication matrices with respect to $[x_1]$ and $[x_2]$ equals

$$A_{x_1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } A_{x_2} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}.$$

It is customary to write A_{x_i} instead of $A_{[x_i]}$ and we will do so in the sequel.

When it comes to rings of projective dimension zero, we have a problem since these rings are infinite dimensional. In order to overcome this problem, we use the graded property among these rings. So let ϕ be defined from R_d to $R_{d+|f|}$ by multiplication by a form f with respect to the bases e_1, \dots, e_m and $f_1, \dots, f_{m'}$ for R_d and $R_{d+|f|}$ respectively. Then A_f (or A_ϕ) is the *projective multiplication matrix* in degree d with respect to f . We will later show that it is possible to choose bases such that the projective multiplication matrices agrees for all degrees greater than or equal to $\text{nz}(R)$.

Example 2.3. For the ring R^u from Example 2.1, we can choose $[x_1^2], [x_1 x_2], [x_2^2]$ as a \mathbb{k} -basis in degree two and $[x_1^3], [x_1^2 x_2], [x_2^3]$ as a \mathbb{k} -basis in degree three. If ϕ denotes the map from R_2^u to R_3^u induced by multiplication by $[x_2]$, then the projective multiplication matrix of degree two with respect to $[x_2]$ equals

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

since $[x_2][x_1^2] = 0[x_1^3] + 1[x_1^2 x_2] + 0[x_2^3]$, $[x_2][x_1 x_2] = 0[x_1^3] + 0[x_1^2 x_2] + 1[x_2^3]$ and $[x_2][x_2^2] = 0[x_1^3] + 0[x_1^2 x_2] + 1[x_2^3]$.

3 Projective multiplication matrices

We will use the fact that rings of projective dimension zero postulates in order to define the projective multiplication matrices.

3.1 Non-zero divisors of degree one

If $p_i = (p_{i0} : \cdots : p_{in})$ is a projective point with respect to the coordinates x_0, \dots, x_n , then we cannot define evaluation on a form in a unique way since $\lambda p_i = p_i$ for non-zero λ . For practical purposes it is however good to define the evaluation in a unique way and we will do this by simply fixing a representation of each projective point. So we associate to each projective point $p_i = (p_{i0} : \cdots : p_{in})$ an affine point $p_i^a = (p_{i0}, \dots, p_{in})$ and now we can define the unique evaluation as $x_0^{\alpha_0} \cdots x_n^{\alpha_n}(p_i) = x_0^{\alpha_0} \cdots x_n^{\alpha_n}(p_i^a) = p_{i0}^{\alpha_0} \cdots p_{in}^{\alpha_n}$. This way of thinking of evaluation is implicit in [18].

With this evaluation method it follows that if l_1 and l_2 are elements of S and $[l_1] = [l_2]$ in R , then $l_1(p) = l_2(p)$ for all points p on $V(I)$. This property makes it possible to define evaluation on elements in R by $[l](p) = l(p)$, where $p \in V(I)$.

We will need a notation for evaluating a set of points on a set of elements. If $P = \{p_1, \dots, p_m\}$ is a set of projective points, we write $f(P) = (f(p_1), \dots, f(p_m))$. If $F = \{f_1, \dots, f_s\}$ is a set of forms in S , then $F(P)$ is defined to be the $(s \times m)$ -matrix whose i 'th row is $f_i(P)$.

Lemma 3.1. *Let I be an ideal of projective dimension zero. Suppose that $V(I) = \overline{V(I)}$. That $[l]$ is a non-zero divisor on R^u is equivalent to $l(p) \neq 0$ for all $p \in V(I)$.*

Proof. Suppose that $l(p) \neq 0$ for all $p \in V(I)$. If $[a] \in R^u$ is such that $[a] \cdot [l] = 0$ in R^u , then $a \cdot l \in I^u$, so that $(a \cdot l)(p) = a(p) \cdot l(p) = 0$ for all $p \in V(I)$. Hence $a(p) = 0$ for all $p \in V(I)$. Thus $a \in I$, so $[l]$ is a non-zero divisor on R^u .

Suppose instead that $[l]$ is a non-zero divisor on R^u . Let q be an arbitrary point in $V(I)$. Let $[Q]$ be an element in R^u such that $Q(q) \neq 0$ and $Q(p) = 0$ for $p \in V(I) \setminus \{q\}$. (The element Q is called a separator for the point q with respect to $V(I)$. Separators exist, see for instance [1] or Section 4.4.1.) Suppose that $l(q) = 0$. Then $Q(p) \cdot l(p) = 0$ for all $p \in V(I)$, so that $[Q] \cdot [l] = 0$. Since $[Q] \neq 0$, it follows that $[l]$ is a zero-divisor, which is a contradiction. Hence $l(p) \neq 0$ for all $p \in V(I)$. \square

Proposition 3.2. *Suppose that \mathbb{k} contains at least $|\overline{V(I)}|$ elements. Then R has a linear non-zero divisor if and only if I is unmixed. The requirement on \mathbb{k} is sharp in the sense that if \mathbb{k} contains $|\overline{V(I)}| - 1$ elements, then there exists an unmixed ideal I such that R lacks linear non-zero divisors.*

Proof. If I is mixed, then R does not contain non-zero divisors. So suppose that I is unmixed. Let $s = |\overline{V(I)}|$ and let $I = \overline{Q_1} \cap \cdots \cap \overline{Q_s}$ be a primary decomposition with respect to \overline{S} . Let $\overline{P_i} = \sqrt{\overline{Q_i}}$. Each $\overline{P_i}$ is generated in degree one. The set of zero-divisors in \overline{R} equals the union of the residues of the $\overline{P_i}$'s (Proposition 4.7 in [2]). So if we let $\overline{NZ} = \overline{S_1} \setminus \cup \overline{P_i}$, then the set of linear non-zero divisors in \overline{R} is the residues of \overline{NZ} . Let $NZ = S_1 \cap \overline{NZ}$. Then the linear non-zero divisors of R is the residues of NZ . Let $\eta_i = \overline{P_i} \cap S_1$.

Suppose that \mathbb{k} is infinite or finite and contains $|\mathbb{k}| \geq s$ elements. Suppose that $v_i \in S_1$ but $v_i \notin \eta_1 \cup \cdots \cup \eta_i$ for $i < s$ (clearly v_1 exists). If $v_i \notin \eta_{i+1}$, then let $v_{i+1} = v_i$. Otherwise, take an element $w_i \in \eta_i$ such that $w_i \notin \eta_{i+1}$ (such an element must exist, since we assume that $v_i \notin \eta_{i+1}$). The element $v_i + \alpha w_i$ does neither belong to η_i nor to η_{i+1} for any non-zero $\alpha \in \mathbb{k}$. Pick $\alpha_1 \in \mathbb{k} \setminus \{0\}$. If $v_i + \alpha_1 w_i \in \eta_{i-1}$, then $v_i + \alpha w_i \notin \eta_{i-1}$ for all $\alpha \in \mathbb{k} \setminus \{\alpha_1\}$, since otherwise

we would have $\alpha(v_i + \alpha_1 w_i) - \alpha_1(v_i + \alpha w_i) = (\alpha - \alpha_1)v_i \in \eta_{i-1}$, which is a contradiction. So pick $\alpha_2 \in \mathbb{k} \setminus \{\alpha_1\}$. Clearly $\eta_i + \alpha_2 w_i \notin \eta_{i-1} \cup \eta_i \cup \eta_{i+1}$. It is clear that we can continue in this way provided that there is at most $i - 1$ non-zero elements in \mathbb{k} . Since i ranges from 1 to s , this construction uses at most $s - 1$ non-zero elements in \mathbb{k} .

Suppose instead that \mathbb{k} is a field with elements $\{a_0, a_1, a_2, \dots, a_{s-1}\}$ with $a_0 = 0$ and $a_1 = 1$. Consider the points $p_1 = (1 : 0 : \dots : 0)$, $p_2 = (1 : 1 : 0 : \dots : 0)$, $p_3 = (1 : a_2 : 0 : \dots : 0)$, \dots , $p_s = (1 : a_{s-1} : 0 : \dots : 0)$ and $p_{s+1} = (0 : 1 : 0 : \dots : 0)$ in $P^n(\mathbb{k})$. Let $I(p_i)$ be the vanishing ideal with respect to p_i , which is prime. Let $I = \cap_i I(p_i)$ and let $l = b_0 x_0 + \dots + b_n x_n$ be an arbitrary linear form. If l is non-zero on p_1, \dots, p_s , then $b_0 + b_1 a_0 \neq 0$, $b_0 + b_1 a_1 \neq 0, \dots, b_0 + b_1 a_{s-1} \neq 0$. Now b_1 must equal zero, since otherwise we would have $b_0 + b_1 a_i \neq b_0 + b_1 a_j$ when $i \neq j$ and thus, by the pigeonhole principle, $b_0 + b_1 a_i = 0$ for some i , which contradicts the assumption that $l(p_i) \neq 0$. But if $b_1 = 0$, then $l(p_{s+1}) = 0$. Thus, the ring lacks linear non-zero divisors by Lemma 3.1. \square

Example 3.1. Let $I = (x_0 + x_1, x_0 + x_2) \cap (x_0 + x_1, x_0 + 2x_2) \cap (x_0 + 2x_1, x_0 + 2x_2) \subseteq Z_3[x_0, x_1, x_2]$. We have $V(I) = \{(1 : 2 : 2), (1 : 2 : 1), (1 : 1 : 1)\}$. To compute a non-zero divisor, we start by computing v_1 . We pick an element of degree one in $(x_0 + x_1, x_0 + x_2)$, say $x_0 + x_1$. By changing one of the coefficients, we can assure that this element is not in $(x_0 + x_1, x_0 + x_2)$, so we let $v_1 = x_0 + 2x_1$. Since $v_1(p_2) \neq 0$ we let $v_2 = v_1$. But $v_2(p_3) = 0$, so we look for an element w_2 which is in $(x_0 + x_1, x_0 + 2x_2)$ but not in $(x_0 + 2x_1, x_0 + 2x_2)$. It is clear that we can find such an element by going through the generators of $(x_0 + x_1, x_0 + 2x_2)$ until we find an element which is not in p_3 . Indeed, $w_2 = x_0 + x_1$ is such an element. We have $v_2 + w_2 = 2x_0$. Since $2x_0(p_1) \neq 0$ we can use $[2x_0]$ (or rather $[x_0]$) as a non-zero divisor.

When \mathbb{k} is finite, it is an interesting question to determine, given a degree d , the maximal number of points allowed to guarantee the existence of a non-zero divisor of degree d . Using a result due to Chevalley, one can show that there is always a non-zero divisor of degree n , even if all points in $P^n(\mathbb{k})$ are considered. However, we will only use non-zero divisors of degree one in this paper and this problem will be dealt with in a separate paper [13].

Proposition 3.3. *Let I be an ideal of projective dimension zero. Suppose that \mathbb{k} contains at least $|V(I)|$ elements. Then there exists a linear form $l \in S_1$ such that $\mathfrak{L} : R_d \rightarrow R_{d+1}, [a] \mapsto [l][a]$ is onto, for all $d \geq \text{nz}(R)$.*

Proof. If $R = R^u$, then, by Proposition 3.2, R contains a nonzero-divisor of degree one which has the desired property. Otherwise, the maximal ideal is associated to I . Thus, the primary decomposition of I can be written as $I = J \cap Q$, with $\sqrt{Q} = \mathfrak{m}$. Let $d \geq \text{nz}(R)$. Then $\dim_{\mathbb{k}}(R_d) = \dim_{\mathbb{k}}(R_d^u)$, which is equivalent to $\dim_{\mathbb{k}}(J_d) = \dim_{\mathbb{k}}(J \cap Q)_d$. Since $(J \cap Q)_d \subseteq J_d$, it follows that $J_d = (J \cap Q)_d$. So that l is a nonzero-divisor on $\oplus_{i \geq d} R_d^u$ implies that l is a nonzero-divisor on $\oplus_{i \geq d} R_d$. \square

Suppose that $\{[e_1], \dots, [e_m]\}$ is a basis for the \mathbb{k} -space $R_d, d \geq \text{nz}(R)$. Since the map induced by l is onto, the set $\{[e_1 l], \dots, [e_m l]\}$ forms a \mathbb{k} -basis for R_{d+1} .

In general, for any positive integer i , $\{[e_1 l^i], \dots, [e_m l^i]\}$ can be chosen as \mathbb{k} -basis for R_{d+i} . This shows the following important theorem.

Theorem 3.4. *Let I be an ideal of projective dimension zero. Let $\{e_1, \dots, e_m\}$ be a \mathbb{k} -basis for R_{nz} . Suppose that R^u has a non-zero divisor $[l]$ of degree one. Then $\{[e_1 l^i], \dots, [e_m l^i]\}$ is a \mathbb{k} -basis for $R_{\text{nz}+i}$, for all positive integers i . The matrix multiplication matrix A_j representing the map $R_{\text{nz}+i} \rightarrow R_{\text{nz}+i+1}$, $[a] \mapsto [x_j a]$ with respect to the bases above, is independent of the choice of i .*

3.2 An affine connection

To a ring R of projective dimension zero, we will now associate an affine ring of dimension zero — R_* , whose multiplication matrices coincide with the projective multiplication matrices of the projective ring. In fact, the zero-dimensional ring R_* is simply $R/([l] - [1])$. The key is the following lemma.

Lemma 3.5. *Suppose that \mathbb{k} contains at least $|\overline{V(I)}|$ elements. Then there is a linear change of coordinates T and a variable x_i such that $T(x_i)(p) \neq 0$ for all points $p \in V(I)$.*

Proof. Let l be the form from proposition 3.3. We can write $l = b_0 x_0 + \dots + b_n x_n$. Some coefficient is non-zero, say $b_i \neq 0$. Let $T(x_i) = l$ and let $T(x_j) = x_j$ if $j \neq i$. \square

Remark 1. *With T as above, if we let $y_0 = T(x_i), y_1 = T(x_0), y_2 = T(x_1), \dots, y_i = T(x_{i-1}), y_{i+1} = T(x_{i+1}), \dots, y_n = T(x_n)$, then each point on $V(I)$ with respect to y_0, \dots, y_n can be written as $(1 : a_1 : \dots : a_n)$.*

Let J be an ideal of affine dimension zero and let $J = q_1 \cap \dots \cap q_s$ be a minimal primary decomposition. The multiplicity of a point $p \in V(J)$, belonging to the primary component $\sqrt{q_i}$, is defined as the length of q_i .

The same definition holds for projective points, that is, if I is an ideal of projective dimension zero and $I = q_1 \cap \dots \cap q_s$, then the multiplicity of a point $p \in V(I)$ belonging to the primary component $\sqrt{q_i}$, is defined as the length of q_i .

These two multiplicity definitions are connected in the sense that if $p = (1 : a_1 : \dots : a_n)$ is a projective point with multiplicity r in $V(I)$, then (a_1, \dots, a_n) is an affine point with multiplicity r in $V(I + (y_0 - 1))$. This is a standard result and treated in [10] and [14] for instance.

Lemma 3.6. *Let I be an ideal of projective dimension zero. Suppose that there exists an $l \in S_1$ such that $[l]$ is a non-zero divisor on R^u . Put $R_* = R/([l] - [1])$. Let $\{[e_1], \dots, [e_m]\}$ be a \mathbb{k} -basis for R_d , for $d \geq \text{nz}(R)$. Then $\{[[e_1]], \dots, [[e_m]]\}$ is a \mathbb{k} -basis for R_* , where $[[\]]$ denotes an equivalence class in $R \bmod [l] - [1]$.*

Proof. Since the \mathbb{k} -dimension of $R/([l] - [1])$ and R_{nz} is determined by the sum of the points counting multiplicity, we have $\dim_{\mathbb{k}}(R/([l] - [1])) = \dim_{\mathbb{k}}(R_{\text{nz}}) = m$. Since $[l]$ is a non-zero divisor on the basis R_{nz} , the vectors $[[e_1]], \dots, [[e_m]]$ are linearly independent. \square

Proposition 3.7. *Let I be an ideal of projective dimension zero. Suppose that \mathbb{k} contains at least $|\overline{V(I)}|$ elements. Let $m = \dim_{\mathbb{k}}(R_{\text{nz}})$. Put $R_* = R/([l] - [1]) = S/(I + ([l] - [1]))$, where l is a non-zero divisor of degree one on R^u . Let*

$\{[e_1 l^i], \dots, [e_m l^i]\}$ be a \mathbb{k} -basis for R_{d+i} and let $\{[[e_1]], \dots, [[e_m]]\}$ be a \mathbb{k} -basis for R_* , where $[[\]]$ denotes an equivalence class in $R \bmod [l-1]$. Then there is a change of coordinates such that the multiplication matrices with respect to x_1, \dots, x_n coincides for R_* and R .

Proof. By a change of coordinates in accordance with Remark 1, we may assume that $l = y_0$. Let $A_k = (a_{ij})$ be the projective multiplication matrix of R with respect to y_k , such that $[y_k][e_i] = a_{i1}[y_0 e_1] + \dots + a_{im}[y_0 e_m]$. It follows that $[[y_k]][[e_i]] = a_{i1}[[e_1]] + \dots + a_{im}[[e_m]]$. By Lemma 3.6, $\{[[e_1]], \dots, [[e_m]]\}$ is a \mathbb{k} -basis for R_* . Hence A_k is the multiplication matrix of R_* with respect to y_k . \square

3.3 Computing the variety from the projective multiplication matrices

We now state the result of Möller and Stetter in the affine setting. See [16] for a proof.

Theorem 3.8. *Let I be a zero dimensional ideal. Let $\{[e_1], \dots, [e_m]\}$ be a \mathbb{k} -basis of $\mathbb{k}[x_1, \dots, x_n]/I$. Let A_1, \dots, A_n be the multiplication matrices with respect to this basis. Let $r = |V(I)|$. Then there are exactly r common (right) eigenvectors for the matrices A_1, \dots, A_n and they are $(e_1(p_i), \dots, e_m(p_i))^t$ for $i = 1, \dots, r$. Let λ_{ij} denote the eigenvalue of A_j corresponding to the eigenvector $(e_1(p_i), \dots, e_m(p_i))^t$. Then $p_i = (\lambda_{i1}, \dots, \lambda_{im})$.*

We have an almost identical theorem in the projective setting.

Theorem 3.9. *Let $I \subseteq \mathbb{k}[x_0, \dots, x_n]$ be an ideal of projective dimension zero. Suppose that \mathbb{k} contains at least $|V(I)|$ elements. Let $\{[e_1], \dots, [e_m]\}$ be a \mathbb{k} -basis of R_{nz} and let l be a linear form such that $\{[e_1 l], \dots, [e_m l]\}$ is a \mathbb{k} -basis for $R_{\text{nz}+1}$. Let A_0, \dots, A_n be the projective multiplication matrices with respect to this basis. Let $r = |V(I)|$. Then there are exactly r common (right) eigenvectors for the matrices A_0, \dots, A_n and they are $(e_1(p_i), \dots, e_m(p_i))^t$ for $i = 1, \dots, r$. Let λ_{ij} denote the eigenvalue of A_j corresponding to the eigenvector $(e_1(p_i), \dots, e_m(p_i))^t$. Then $p_i = (\lambda_{i0} : \lambda_{i1} : \dots : \lambda_{im})$.*

Proof. By Proposition 3.3, there exists a linear form $l = b_0 x_0 + \dots + b_n x_n$ such that $\{[e_1 l], \dots, [e_m l]\}$ forms a \mathbb{k} -basis for $R_{\text{nz}+1}$. By Remark 1, there is a change of coordinates such that the multiplication matrix B_i with respect to y_i satisfies $B_0 = b_0 A_0 + \dots + b_n A_n$ and $B_1 = A_0, B_2 = A_1, \dots, B_i = A_{i-1}, B_{i+1} = A_{i+1}, \dots, B_n = A_n$.

By Proposition 3.7, the projective multiplication matrices B_1, \dots, B_m of R with respect to y_1, \dots, y_m agree with the multiplication matrices for $R/(l-1)$ with respect to y_1, \dots, y_m .

Since the multiplication matrix with respect to y_0 is the identity, a common eigenvector for B_1, \dots, B_n is also a common eigenvector for B_0, \dots, B_n and vice versa. But by linearity, v is a common eigenvector to B_0, \dots, B_n if and only if v is an eigenvector to A_0, \dots, A_n . Hence, the set of common eigenvectors for A_0, \dots, A_n equals $e_1(p_i), \dots, e_m(p_i)$, for $i = 1, \dots, r$, by Theorem 3.8. \square

To determine the multiplicity of a point $p \in V(I)$, one can use the result of Corless et al in [5]. The method goes as follows. Let A be a generic linear

combination of the multiplication matrices. Let λ be the eigenvalue of A with respect to $e(p)$ (clearly $e(p)$ is an eigenvector of A). Then the multiplicity of p equals the algebraic multiplicity of λ . There are also direct methods which one could use, see for instance [15] and [17].

Example 3.2. The elements

$$\begin{aligned} f_1 &= xz + yz - z^2 \\ f_2 &= x^2 - y^2 + 2yz - z^2 \\ f_3 &= xy - y^2 + yz \end{aligned}$$

generates an unmixed ideal I of projective dimension zero in $\mathbb{C}[x, y, z]$. Choosing $[x], [y], [z]$ and $[y^2], [yz], [z^2]$ as bases in degree 1 and 2 respectively, we see that neither $[x]$, $[y]$ nor $[z]$ serve as nonzero-divisors. Indeed, if we let M_x, M_y and M_z denote the multiplication matrices from R_1 to R_2 with respect to the bases chosen above, we compute

$$M_x = \begin{pmatrix} 1 & -2 & 1 \\ 1 & -1 & 0 \\ 0 & -1 & 1 \end{pmatrix}, M_y = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, M_z = \begin{pmatrix} 0 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

and we can see that all the matrices have a nontrivial kernel. However, $M_y + M_z$ has full rank which is equivalent to $[y + z]$ being a nonzero-divisor. Hence, if we use $\{[x(y + z)], [y(y + z)], [z(y + z)]\}$ as a \mathbb{k} -basis in degree two, we can construct the projective multiplication matrices A_x, A_y and A_z . From these matrices the solutions can be read off. Now $[x(y + z)] = [y^2] - 2[zy] + [z^2]$, $[y(y + z)] = [y^2] + [zy]$, $[z(y + z)] = [yz] + [z^2]$ by making use of the multiplication matrices above. Thus, with

$$T = \begin{pmatrix} 1 & 1 & 0 \\ -2 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

we have

$A_x = M_x(T^t)^{-1}$ and similarly for A_y and A_z , so that

$$A_x = \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}, A_y = \frac{1}{4} \begin{pmatrix} 2 & 2 & -2 \\ 1 & 3 & -1 \\ -1 & 1 & 1 \end{pmatrix},$$

and

$$A_z = \frac{1}{4} \begin{pmatrix} 2 & -2 & 2 \\ -1 & 1 & 1 \\ 1 & -1 & 3 \end{pmatrix}.$$

Common eigenvectors for the matrices are $(1, 1, 0)$, $(1, 0, 1)$ and $(0, 1, 1)$. The eigenvalues corresponding to $(1, 1, 0)$ are 1, 1, 0 for A_x, A_y and A_z respectively. Likewise, the eigenvalues corresponding to $(1, 0, 1)$ are 1, 0, 1 and the eigenvalues corresponding to $(0, 1, 1)$ are 0, 1, 1. Thus, $V(I) = \{(1 : 1 : 0), (1 : 0 : 1), (0 : 1 : 1)\}$.

Notice that since $\text{nz}(R) = 1$, we can also use the correspondence between eigenvectors and the \mathbb{k} -basis to obtain the points. Indeed $([x](p_1), [y](p_1), [z](p_1)) = (1, 1, 0)$, thus we have $p_1 = (1 : 1 : 0)$, etc.

4 Applications and computational aspects

A convenient way to think of a ring $R = S/I$ of projective dimension zero is as

$$\tilde{R} = R_0 \oplus R_1 \oplus \cdots \oplus R_{nz}$$

together with the linear map l and the multiplication matrices A_1, \dots, A_n . We write this information as a triplet (\tilde{R}, A, l) . The \mathbb{k} -dimension of the graded pieces of \tilde{R} describes the configuration of the points and also tells whether or not the maximal ideal is associated, while the multiplication matrices encode the variety as a set. In Section 4.1 we will see that we obtain a fast normal form algorithm by using the triplet. With this perspective, the classical way of determining a Gröbner basis for I misses a lot of information about the ring. It also turns out that we compute unnecessary data. For instance, a Gröbner basis for the ideal $I = (xz + yz - z^2, x^2 - y^2 + 2yz - z^2, xy - y^2 + yz)$ from Example 3.2 with respect to $x > y > z$ and DegRevLex is $(xz + yz - z^2, x^2 - y^2 + 2yz - z^2, xy - y^2 + yz, y^2z - yz^2)$. Since $\text{nz}(R) = 1$, we only need to consider the \mathbb{k} -spaces R_1 and R_2 to determine the variety, and for this purpose, the term $y^2z - yz^2$ in the Gröbner basis is superfluous. In Section 4.2 we will show that the maximal degree of a term in a Gröbner basis is $\max(\text{nz}(R), m)$. Since it is enough to compute up to degree $\text{nz}(R)$ in order to determine the variety, this indicates that Gröbner techniques are not always optimal. Unfortunately, it is hard to detect $\text{nz}(R)$.

4.1 Computing normal forms with respect to (\tilde{R}, A, l)

As an application of the multiplication matrices, we obtain a fast normal form algorithm for high degree elements of S . Suppose that we have a normal form algorithm $\text{Nf}(*, B)$ for elements of degree less than or equal to $\text{nz}(R)$. To extend this method to elements of degree $> \text{nz}(R)$, we proceed as follows. Let $a \cdot b$ be a monomial in S and suppose that $|b| = \text{nz}(R)$. We use the normal form algorithm for low degree elements to obtain $\text{Nf}(b, B) = b_1e_1 + \cdots + b_me_m$. To determine $\text{Nf}(ab, B)$, write $a = x_1^{a_1} \cdots x_n^{a_n}$. It is straightforward to check that

$$\text{Nf}(ab, B) = (b_1, \dots, b_m) A_1^{a_1} \cdots A_n^{a_n} (l^{|a|}e_1, \dots, l^{|a|}e_m)^t.$$

Thus, the arithmetic complexity of the normal form algorithm is $O(|a|m^3)$ if one uses naive matrix multiplication or $O(|a|m^{2.376})$ if one uses state of the art methods [4]. To this one needs to add the complexity for computing $\text{Nf}(b, B)$.

Example 4.1. Suppose that we want to compute the normal form of x^{17} with respect to the ideal I from Example 3.2. We have seen that $\{[x(y+z)^i], [y(y+z)^i], [z(y+z)^i]\}$ forms a \mathbb{k} -basis for R/I and that

$$A_x = \frac{1}{2} \begin{pmatrix} 2 & 0 & 0 \\ 1 & 1 & -1 \\ 1 & -1 & 1 \end{pmatrix}.$$

Since $[x]$ is a basis element in degree one, the normal form of x^{17} equals

$$(1, 0, 0) A^{16} (x(y+z)^{16}, y(y+z)^{16}, z(y+z)^{16})^t.$$

Since $A^2 = 2 \cdot A$, we have $A^{16} = 2^{15}A$. Hence

$$\text{Nf}(x^{17}, x(y+z)^{16}, y(y+z)^{16}, z(y+z)^{16}) = 2^{15}x(y+z)^{16}.$$

If we know the variety of I , then the normal form computation can be simplified, see Example 4.4.

4.2 Upper bound of the elements in a Gröbner basis

To give an upper bound of the maximal degree of an element in a Gröbner basis with respect to an ideal of projective dimension zero, we will use Gotzmann's persistence theorem.

Recall that if h and i are positive integers, then h can be uniquely written as a sum

$$h = \binom{n_i}{i} + \binom{n_{i-1}}{i-1} + \cdots + \binom{n_j}{j},$$

where

$$n_i > n_{i-1} > \cdots > n_j \geq j \geq 1.$$

See [18] for an easy proof. This sum is called the binomial expansion of h in base i . Define

$$h^{<i>} = \binom{n_i+1}{i+1} + \binom{n_{i-1}+1}{i} + \cdots + \binom{n_j+1}{j+1}.$$

Before stating Gotzmann's theorem, recall that the Hilbert function of a graded algebra R is the map $d \mapsto \dim_{\mathbb{k}}(R_d)$.

Theorem 4.1 (Gotzmann's persistence theorem [9]). *Let Hf be the Hilbert function of $k[x_1, \dots, x_n]/I$, for any homogeneous ideal I . Let t denote the maximal degree of the generators of I . Then $\text{Hf}(d+1) = \text{Hf}(d)^{<d>}$ for some $d \geq t$ implies that $\text{Hf}(d+2) = \text{Hf}(d+1)^{<d+1>}$, $\text{Hf}(d+3) = \text{Hf}(d+2)^{<d+2>}$ and so on.*

In the case of projective points, we have $\text{Hf}(d+1) = \text{Hf}(d) = m$ when $d \geq \text{nz}(R)$, thus we have $\text{Hf}(d+1)^{<d+1>} = \text{Hf}(d)^{<d>} = m$ for $d \geq \text{nz}(R)$ and hence

$$\text{Hf}(d)^{<d>} = \binom{d+1}{d+1} + \cdots + \binom{d-(m-2)}{d-(m-2)}.$$

A Lex-segment set L_d on $\{x_1, \dots, x_n\}$ is the $|L_d|$ biggest monomials of degree d in $\mathbb{k}[x_1, \dots, x_n]$ with respect to the lexicographical ordering. When L is a collection of Lex-segment sets, let $I(L)$ denote the ideal generated by the elements in the Lex-segment sets. We call $I(L)$ a Lex-segment ideal. When I is a homogeneous ideal, let $|\text{in}(I)_d^c|$ denote the number of monomials outside $\text{in}(I)$ of degree d . Notice that $|\text{in}(I)_d^c|$ is independent of monomial ordering.

Let I be a homogeneous ideal generated in degree less than or equal to d and let L be a collection of Lex-segment sets with maximal degree d . A property among Lex-segment ideals is that they have minimal growth (or maximal co-growth), in the sense that if $|\text{in}(I)^c|$ and $|\text{in}(I(L))^c|$ agrees until degree d , then

$$|\text{in}(I(L))_{d'}^c| \geq |\text{in}(I_{\leq d})_{d'}^c| \text{ for all } d' \geq d.$$

See for instance [18].

Theorem 4.2. *Let I be an ideal of projective dimension zero. A bound for the maximal degree of an element in a reduced Gröbner basis is $\max(\text{nz}(R), m)$.*

Proof. Let $d = \max(\text{nz}(R), m)$. Suppose that L is a collection of Lex-segment sets of degrees less than or equal to d , such that $|\text{in}(I(L))^c|$ agrees with $|\text{in}(I)^c|$ until degree d . We then have

$$m = |\text{in}(I(L))_{d'}^c| \geq |\text{in}(I_{\leq d})_{d'}^c| \geq |\text{in}(I_{\leq d'})_{d'}^c| = m.$$

This implies that $|\text{in}(I_{\leq d})_{d'}^c| = |\text{in}(I_{\leq d'})_{d'}^c|$ for all $d' \geq d$ and hence there can not be any Gröbner basis element of degree greater than d . \square

This theorem is a generalization of the result in [1], where it is shown that the last degree element of a Gröbner basis is m in the case when I is unmixed. The bound in Theorem 4.2 is sharp. Indeed, in Example 3.2, $\text{nz}(R) = 1, m = 3$ and a reduced Gröbner basis with respect to DegRevLex had a generator in degree three, while in Example 4.2 below, we will see that $\text{nz}(R) = 3, m = 1$ and a reduced Gröbner basis with respect to DegRevLex is $\{xy - z^2, x^2 - xz, y^2 - z^2, xz^2 - yz^2, -yz^2 + z^3\}$.

4.3 Computing (\tilde{R}, A, l) given the ideal

Suppose that we are given an ideal by its generators and that we know that $\dim_{\mathbb{k}}(R_d) = \dim_{\mathbb{k}}(R_{d+1})$ for some d . What conclusions can be made from this information? Unfortunately, not many. We do not know the dimension — indeed — the rings $\mathbb{k}[x, y, z]/(xy, yz, xz)$, $\mathbb{k}[x, y, z]/(x^2, y^2, z^2)$ and $\mathbb{k}[x, y, z]/(x^2, xy, xz)$ all have \mathbb{k} -dimension three in degrees one and two. The first ring is of projective dimension zero and postulates in degree one. The second ring is artinian, while the third ring is of projective dimension one. However, we have the following simple observation.

Lemma 4.3. *Let I be a graded ideal in S and suppose that there is an element $[f] \in R_i$ such that $[f]R_d = R_{d+i}$. Then R is either artinian or of projective dimension zero.*

Proof. The ring $S/(I + (f))$ is artinian, hence S/I is of at most projective dimension zero. \square

Lemma 4.4. *Suppose that $(f_1, \dots, f_n) = I$ is generated by n elements in $\mathbb{k}[x_0, \dots, x_n]$ and that there is an element $[f] \in R_i$ such that $[f]R_d = R_{d+i}$. Then R is of projective dimension zero.*

Proof. The ring $S/(I + (f))$ is artinian, hence (f_1, \dots, f_n, f) forms a regular sequence. But also (f_1, \dots, f_n) forms a regular sequence, so S/I is of projective dimension zero. \square

Even if we know that R is of projective dimension zero, it is also hard to tell whether or not the maximal ideal is associated. The following example shows that although $\dim_{\mathbb{k}}(R_d) = \dim_{\mathbb{k}}(R_{d+1})$ and there is an element l such that $[l]R_d = R_{d+1}$, it does not hold that $d \geq \text{nz}(R)$.

Example 4.2. Let $I = (x^2 - xz, xy - z^2, y^2 - z^2)$. Then $\text{Hs}(R, t) = 1 + 3t + 3t^2 + t^3 + t^4 + \dots$ and $\text{nz}(R) = 3$. We have $I = (x - y, x - z) \cap (z^2, y^2, xy, x^2 - xz)$, $V(I) = V((x - y, x - z)) = (1 : 1 : 1)$ and $\sqrt{(z^2, y^2, xy, x^2 - xz)} = (x, y, z)$. We can choose $\{[x], [y], [z]\}$ and $\{[xz], [yz], [z^2]\}$ as \mathbb{k} -bases in degree one and two respectively and thus, the map from R_1 to R_2 induced by multiplication by $[z]$ is injective.

Fortunately, as the next theorem shows, if we are only interested in computing the variety, it is enough to find an l such that $[l]R_d = R_{d+1}$.

Theorem 4.5. *Let I be any homogeneous ideal and let $R = S/I$. Suppose that there exists an element $[l]$ such that $[l]R_d = R_{d+1}$. Let $[f_1], \dots, [f_t]$ be a \mathbb{k} -basis for R_{d+1} . Let $[e_1], \dots, [e_t]$ be such that $[e_i][l] = [f_i]$. Let A_0, \dots, A_n be such that A_i corresponds to multiplication with x_i with respect to the bases $[e_1], \dots, [e_t]$ and $[f_1], \dots, [f_t]$.*

Suppose that $p \in V(I)$. Then $e(p)^t = (e_1(p), \dots, e_t(p))^t$ is a common eigenvector to the A_i 's. Let λ_i be the eigenvalue of A_i corresponding to $e(p)^t$. Then $p = (\lambda_0 : \lambda_1 : \dots : \lambda_n)$.

Proof. By the definition of the matrix A_j we have

$$[x_j][e_k] = a_{k1}^{(j)}[le_1] + \dots + a_{kt}^{(j)}[le_t].$$

Thus, we get

$$x_j(p)e_k(p) = a_{k1}^{(j)}l(p) \cdot e_1(p) + \dots + a_{kt}^{(j)}l(p) \cdot e_t(p),$$

or put in matrix form

$$x_j(p)e(p)^t = A_j l(p)e(p)^t. \quad (1)$$

Now $e(p)^t$ can not be the zero vector, since otherwise we would have $p \in V(I + (e_1) + \dots + (e_t))$, which is a contradiction since $S/(I + (e_1) + \dots + (e_t))$ is artinian. With the same argument, $l(p)$ must be non-zero.

Hence $\frac{e(p)^t}{l(p)}$ is an eigenvector of A_j with the eigenvalue $\frac{x_j(p)}{l(p)}$. The theorem follows since

$$\begin{aligned} (\lambda_0 : \lambda_1 : \dots : \lambda_n) &= (x_0(p)/l(p) : x_1(p)/l(p) : \dots : x_n(p)/l(p)) \\ &= (x_0(p) : x_1(p) : \dots : x_n(p)). \end{aligned}$$

□

Example 4.3. Let $I = (y^2, z^2, xz, xy)$. Then $\dim_{\mathbb{k}}(R_1) = 3$ and $\dim_{\mathbb{k}}(R_2) = 2$. We can choose $[x], [y], [z]$ and $[x^2], [yz]$ as \mathbb{k} -bases in degrees one and two respectively. It is clear that $[x+z]R_2 = R_3$ and thus, by Lemma 4.3, we know that I is of at most projective dimension zero. We have $[x+z][x] = [x^2]$ and $[x+z][y] = [yz]$, so with respect to the bases $[x], [y]$ and $[x+z][x], [x+z][y]$, we get

$$A_x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, A_y = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ and } A_z = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

There are two common eigenvectors for these matrices — $(1, 0)$ and $(0, 1)$. The associated eigenvalues are $1, 0, 0$ and $0, 0, 1$ respectively. By Theorem 4.5, we know that $V(I) \subseteq \{(1 : 0 : 0), (0 : 0 : 1)\}$. We have $y^2((1 : 0 : 0)) = z^2((1 : 0 : 0)) = xz((1 : 0 : 0)) = xy((1 : 0 : 0)) = 0$, but $z^2((0 : 0 : 1)) \neq 0$, so $V(I) = \{(1 : 0 : 0)\}$. Thus, the second point was "false".

Theorem 4.5 could also be used to compute the variety in Example 4.2. We leave this computation as an exercise to the reader.

So suppose that we want to compute the variety of an ideal I which we suspect is of projective dimension zero. We propose the following procedure for a field \mathbb{k} with enough elements.

- K1** Compute the Gröbner basis elements of degree 1, 2 and so on until we reach a degree d such that $|\text{in}(I)_d^c| \geq |\text{in}(I)_{d+1}^c|$ (this is the same as $\dim_{\mathbb{k}}(R_d) \geq \dim_{\mathbb{k}}(R_{d+1}) = t$).
- K2** Choose a linear form $[l]$ at random and check if $R_d[l] = R_{d+1}$. If it was not, choose another l . If we did not find such an element even after many tries, go back to stage K1 and compute more Gröbner basis elements.
- K3** Choose a basis $\{[f_1], \dots, [f_t]\} = [\text{in}(I)_{d+1}^c]$ for R_{d+1} and let e_1, \dots, e_t be such that $[e_i][l] = f_i$.
- K4** Compute the multiplication matrices with respect to $\{[e_t], \dots, [e_1]\}$ and $\{[f_1], \dots, [f_t]\}$.
- K5** Determine a set of common eigenvectors for these matrices, either by using symbolic or numerical methods and use Theorem 4.5 to determine the variety of I .

We refer the reader to the book [19] and the citations therein for techniques to compute common eigenvectors using numerical methods.

4.4 Computing (\tilde{R}, A, l) from the points

Given a set of projective points $P = \{p_1, \dots, p_m\}$ one can form the vanishing ideal $I(P)$, which consists of all polynomials vanishing on all of the points in P . The Hilbert series of $R/I(P)$ is well studied but not completely understood, cf. [8]. The most common way of computing Hilbert series of an ideal defined by projective points has been studied by means of the projective Buchberger-Möller algorithm [1, 14]. This algorithm computes a Gröbner basis of a vanishing ideal by computing a \mathbb{k} -basis for the \mathbb{k} -spaces R_0, R_1, \dots, R_d until degree $\max(m, \text{nz}(R))$ and reducing potential Gröbner basis elements with respect to this basis. We will present a reduced version of the projective Buchberger-Möller algorithm which instead of computing the Gröbner basis of $I(P)$ computes the triplet (\tilde{R}, A, l) and we will show that the behavior of our method is asymptotically better than the classical Buchberger-Möller-algorithm.

Recall that we suppose that the representation of each projective point is fixed so that we can define evaluation of projective points in a unique way.

A nice way to compute normal forms with respect to vanishing ideals of projective points is by evaluation: Given a form f of degree d and a vector space basis e_1, \dots, e_m of R_d , we obtain the normal form $\alpha_1 e_1 + \dots + \alpha_m e_m$, where the α_i 's are chosen to satisfy $f(p_i) = \alpha_1 e_1(p_i) + \dots + \alpha_m e_m(p_i)$ for $i = 1, \dots, m$. The normal form does not depend on the choice of representation of the points. Computing normal forms by means of evaluation is the key engine behind the graded Buchberger-Möller algorithm and the variation of the method given below.

When studying ideals of projective points, one can always assume that $n + 1 \leq m$. Indeed, we have the following lemma, which is a graded version of Lemma 5.2 in [12].

Lemma 4.6. *Let $E = \{x_{i_0}, \dots, x_{i_{\pi}}\}$ be any subset of the variables such that $E(P)$ and $\{x_0, \dots, x_n\}(P)$ has same rank. Let π be the natural projection from $P^n(\mathbb{k})$ to $P^{\pi}(\mathbb{k})$ defined by $\pi((a_0 : \dots : a_n)) = (a_{i_0} : \dots : a_{i_{\pi}})$. Then q_1, \dots, q_m*

are distinct where $q_i = \pi(p_i)$. Moreover, with $Q = \{q_1, \dots, q_m\}$ and with $\bar{R} = \mathbb{k}[x_{i_0}, \dots, x_{i_{\bar{\pi}}}] / I(Q)$, the graded algebras \bar{R} and R are isomorphic.

Proof. Suppose that $x_i \notin E$. Then $x_i(P) = \alpha_1 x_{i_1}(P) + \dots + \alpha_{\bar{\pi}} x_{i_{\bar{\pi}}}(P)$. Hence $x_i - \alpha_1 x_{i_1} + \dots + \alpha_{\bar{\pi}} x_{i_{\bar{\pi}}} \in I$. Since $R_{\geq 1}$ is generated in degree one, it is clear that the elements in E generates $R_{\geq 1}$. Since the evaluation on q_i 's and the p_i 's agrees on the elements in $\mathbb{k}[x_{i_0}, \dots, x_{i_{\bar{\pi}}}]$, it follows that \bar{R} and R are isomorphic as graded algebras. It is clear that q_1, \dots, q_m are distinct. \square

Remark 2. In a more subtle way, Lemma 4.6 actually follows directly from the projective Buchberger-Möller algorithm.

We now give a variant of the projective Buchberger-Möller algorithm for building the triplet (\tilde{R}, A, l) from the points. As for the Buchberger-Möller algorithm, this algorithm is based on the evaluation method to compute normal forms. But it differs from the Buchberger-Möller algorithm in the sense that it is focused on giving the multiplication tables with respect to the variables rather than giving a Gröbner basis for the ideal.

- L1** Compute a non-zero divisor l of degree one by using the method in Proposition 3.2.
- L2** Initiate the lists $B_0 = L_0 = [1]$ and Initials = \square . Let $d = 0$.
- L3** If $\text{rank}(B_d(P)) = |P|$, then $\text{nz}(R) = d$. Return B_0, \dots, B_d and l . Otherwise, increase d by one, let $B_d = \square$ and let L_d be the list of all monomials of degree d which are not multiples of an element of Initials.
- L4** If L_d is empty, go to step L3; otherwise choose the monomial $t = \min_{\prec}(L_d)$ with respect to a fixed monomial order and remove it from L_d .
- L5** If $t(P)$ can be written as a linear combination of the rows in $B_d(P)$, then add t to the set Initials and continue with step L4. Else, append t to B_d and continue with step L4.

The correctness of the method is a direct consequence of the projective BM-algorithm, since the sets B_0, \dots, B_d are computed in the same way using the two methods. Thus Initials will generate $\text{in}(I)_{\prec}$, while B will be the complement of $\text{in}(I)_{\prec}$. By using another selection method in step L4, it is possible to obtain a basis which is not necessarily the complement of an initial ideal (It is an easy exercise to check that the termination of the algorithm does not depend on the selection method).

We implicitly assume that we have used Lemma 4.6 so that $n \leq m$. This preprocessing can be done using $O(nm^2)$ arithmetic operations, since we test for linear dependence n times. It is straightforward to lift the result in [11] and show that the complexity of the algorithm is dominated by the arithmetic operations and not the monomial manipulations. The number of arithmetic operations for the step L1 is bounded by $O(m^3)$ by an elementary analysis of the method in Proposition 3.2. For each degree d during the algorithm, we need to check linear dependence at most $\min(m, n)m$ times. Thus, the arithmetic complexity of the method is a cost of at most $O(\text{post}(R) \min(m, n)m^3)$. The original analysis [14] of the Buchberger-Möller algorithm reports the complexity $O(nm^4)$. (Although it is possible to show that the performance is $O(\min(m, n)nm^3)$.)

Example 4.4. In Example 3.5 in [1], the point set $P = \{(0 : 2 : 5), (0 : 1 : 2), (1 : 3 : 1), (4 : 3 : 4), (2 : 5 : 4), (1 : 4 : 4)\}$ is considered. The Gröbner basis with respect to DegRevLex and $x \prec y \prec z$ is generated in degrees three and four and $\text{Hs}(R, t) = 1 + 3t + 6t^2 + 6t^3 + \dots$.

With our approach, we would first fix the coordinates $P = \{(0, 2, 5), (0, 1, 2), (1, 3, 1), (4, 3, 4), (2, 5, 4), (1, 4, 4)\}$ and then compute $L_0 = \{1\}$, $B_0 = \{1\}$ and $L_1 = \{x, y, z\}$. Since $\{x, y, z\}(P)$ has full rang, we will have $B_1 = \{x, y, z\}$. Thus, Initials is empty and $L_2 = \{z^2, yz, xz, y^2, xy, x^2\}$. It turns out that also $\{z^2, yz, xz, y^2, xy, x^2\}(P)$ has full rang, so $B_2 = \{z^2, yz, xz, y^2, xy, x^2\}$. Since $|P| = 6$, the algorithm stops and we know that $\text{Hs}(R, t) = 1 + 3t + 6t^2 + 6t^3 + \dots$. It is immediate that $y(p_i) \neq 0$ for $i = 1, \dots, 6$, so we can use $B_3 = \{yz^2, y^2z, xyz, y^3, xy^2, x^2y\}$ as a \mathbb{k} -basis in degree three, and in general

$$B_d = \{y^{d-2}z^2, y^{d-1}z, xy^{d-2}z, y^d, xy^{d-1}, x^2y^{d-2}\}.$$

Say that we want to compute the normal form of $x^6 + z^6$. If we do it by evaluation, we solve the linear equations

$$(x^6 + z^6)(p_i) = (\alpha_1 y^4 z^2 + \alpha_2 y^5 z + \alpha_3 xy^4 + \alpha_4 y^6 + \alpha_5 xy^5 + \alpha_6 x^2 y^4)(p_i)$$

for $i = 1, \dots, 6$ which is equivalent to perform Gaussian elimination on a (6×6) -matrix. As result, we get

$$\begin{aligned} \text{Nf}(x^6 + z^6, B) &= \frac{2083926583}{23522400}y^6 - \frac{11603225231}{470448000}xy^5 - \frac{8111541583}{26136000}y^5z \\ &\quad - \frac{327280970021}{940896000}x^2y^4 + \frac{17527852333}{117612000}y^4z^2 + \frac{127511218609}{313632000}xy^4z. \end{aligned}$$

We could also use the multiplication matrices. Notice that A_x, A_y and A_z share the six linear independent eigenvectors

$$(z^2(p_i), yz(p_i), xz(p_i), y^2(p_i), xy(p_i), x^2(p_i))^t.$$

Thus, if we let $T = B_2(P)^t$, we have $A_x = TD_xT^{-1}$, $A_y = TD_yT^{-1}$ and $A_z = TD_zT^{-1}$, where $D_x = \text{diag}(0, 0, 1/3, 4/3, 2/5, 1/4)$, $D_y = \text{diag}(1, 1, 1, 1, 1, 1)$ and $D_z = \text{diag}(5/2, 2, 1/3, 4/3, 4/5, 1)$.

So to compute the normal form of $x^6 + z^6$, we can start by computing $\text{Nf}(x^2, B) = x^2 = (0, 0, 0, 0, 0, 1) \cdot (z^2, yz, xz, y^2, xy, x^2)$ and $\text{Nf}(z^2, B) = z^2 = (1, 0, 0, 0, 0, 0) \cdot (z^2, yz, xz, y^2, xy, x^2)$. We get $\text{Nf}(x^6 + z^6, B) = \text{Nf}(x^6, B) + \text{Nf}(z^6, B)$, where

$$\begin{aligned} \text{Nf}(x^6, B) &= (0, 0, 0, 0, 0, 1)A_x^4(y^4z^2, y^5z, xy^4z, y^6, xy^5, x^2y^4)^t \\ &= (0, 0, 0, 0, 0, 1)TD_x^4T^{-1}(y^4z^2, y^5z, xy^4z, y^6, xy^5, x^2y^4)^t \end{aligned}$$

and

$$\begin{aligned} \text{Nf}(z^6, B) &= (1, 0, 0, 0, 0, 0)A_z^4(y^4z^2, y^5z, xy^4z, y^6, xy^5, x^2y^4)^t \\ &= (1, 0, 0, 0, 0, 0)TD_z^4T^{-1}(y^4z^2, y^5z, xy^4z, y^6, xy^5, x^2y^4)^t. \end{aligned}$$

Of course, we get the same result as above.

4.4.1 Computing separators

A family of separators with respect to a set of affine points $P = \{p_1, \dots, p_m\}$, is a set $\{f_1, \dots, f_m\}$ of polynomial functions such that $f_i(p_i) = 1$ and $f_i(p_j) = 0$ if $i \neq j$. It is easy to see that the separators forms a \mathbb{k} -basis for $\mathbb{k}[x_1, \dots, x_n]/I(P)$.

When the points are projective, we say that $\{f_1, \dots, f_m\}$ is a set of separators if $f_i(p_i) \neq 0$ and $f_i(p_j) = 0$ when $i \neq j$. When all separators are of the same degree d , they constitute a \mathbb{k} -basis for R_d . If \mathbb{k} contains at least m elements so that there exists a non-zero divisor l , we can construct a separator- \mathbb{k} -basis for R_{d+i} as $f_1 l^i, \dots, f_m l^i$.

In [12], two methods for computing separators with respect to a collection of affine points are discussed. It is possible to lift this method to the projective setting. Both methods perform the same number of arithmetic operations. We will illustrate one of the methods by an example. In \mathbb{Z}^5 , consider $p_1 = (1, 2, 0, 1, 1)$, $p_2 = (1, 0, 1, 1, 2)$, $p_3 = (1, 2, 0, 3, 3)$, $p_4 = (0, 0, 2, 0, 4)$, $p_5 = (0, 0, 2, 1, 5)$ and $p_6 = (2, 1, 3, 1, 6)$. We associate the following table to this point set

$$\left(\begin{array}{ccccc|c} 1 & 1 & 1 & 0 & 0 & 2 \\ 2 & 0 & 2 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 & 2 & 3 \\ 1 & 1 & 3 & 0 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{array} \middle| \begin{array}{l} \Sigma_1 = \{ \{1, 2, 3\}, \{4, 5\}, \{6\} \} \\ \Sigma_2 = \{ \{1, 3\}, \{2\}, \{4, 5\}, \{6\} \} \\ \Sigma_3 = \{ \{1, 3\}, \{2\}, \{4, 5\}, \{6\} \} \\ \Sigma_4 = \{ \{1\}, \{3\}, \{2\}, \{4\}, \{5\}, \{6\} \} \\ \Sigma_5 = \{ \{1\}, \{3\}, \{2\}, \{4\}, \{5\}, \{6\} \} \end{array} \right)$$

The sets on the right hand side are also described by an example: The set $\{1, 3\}$ on the second row shows that p_1 and p_3 agree on the first two coordinates. When computing such a table from a point set, one obtains a matrix c_{ij} , where c_{ij} is the first position where p_i and p_j differ.

This matrix is used to compute the separators and it is clear that

$$Q_i = \prod_{j \neq i} \frac{x_{c_{ij}} - p_{jc_{ij}}}{p_{ic_{ij}} - p_{jc_{ij}}}$$

satisfies $Q_i(p_j) = 0$ if $i \neq j$ and $Q_i(p_i) = 1$.

It is showed in [12] that at most $nm + m^2$ arithmetic comparisons are used to compute the matrix c_{ij} . (In fact a slightly improved upper bound is given.)

We will now show how to make use of the matrix c_{ij} to compute projective separators. If we let $S_{ij}(p_i) \neq 0$ and $S_{ij}(p_j) = 0$, then Q_1, \dots, Q_m is a set of projective separators for p_1, \dots, p_m , where

$$Q_i = \prod_{j \neq i} S_{ij}. \quad (2)$$

Suppose that each point p_i is normalized in the sense that the first non-zero position equals one. It is then clear that we can use the affine method to compute the matrix (c_{ij}) with respect to the points.

We will now give an explicit formula for each S_{ij} . To simplify notation, let $h = c_{ij}$.

- If $p_{ih} = 0$, then $p_{jh} \neq 0$. Let h' be the least position such that $p_{ih'} = 1$ and let $S_{ij} = p_{jh} x_{h'} - p_{jh'} x_h$.
- Else, if $p_{ih} \neq 0$ but $p_{jh} = 0$, then let $S_{ij} = x_h$.

- Finally, suppose that $p_{ih} \neq 0$ and $p_{jh} \neq 0$. Since p_i and p_j agrees on all coordinates less than h and $p_{ih} \neq p_{jh}$, there is a $h' \leq h$ such that $p_{ih'} = p_{jh'} = 1$. Thus, let $S_{ij} = p_{jh}x_{h'} - p_{jh'}x_h = p_{jh}x_{h'} - x_h$.

Notice that we can choose the index h' occurring in the two situations as the first entry where p_i equals one. It is clear that we can determine the first non-zero index of each point using at most nm arithmetic comparisons. We have proved the following theorem.

Theorem 4.7. *Let $P = \{p_1, \dots, p_m\}$ be a set of distinct projective points. Then we can compute a set of separators of degree $m - 1$ with respect to P using at most $nm + m^2$ arithmetic operations.*

Example 4.5. Let $p_1 = (1 : 2 : 0 : 1 : 1 : 0 : 3 : 5)$, $p_2 = (1 : 0 : 1 : 1 : 2 : 0 : 3 : 5)$, $p_3 = (1 : 2 : 0 : 3 : 3 : 1 : 2 : 0)$ and let $p_4 = (0 : 1 : 1 : 0 : 2 : 0 : 1 : 0)$. We will show how to compute Q_1 . We have $c_{12} = 2$ and $p_{12} = 2$ and $p_{22} = 0$. Thus, $S_{12} = x_2$. We have $c_{13} = 4$ and $p_{14} = 1$ and $p_{34} = 3$. Since $p_{11} = p_{31} = 1$, we let $S_{13} = p_{34}x_1 - x_4 = 3x_1 - x_4$. We have $c_{14} = 1$ and $p_{41} = 0$, so $S_{14} = x_1$. Hence $Q_1 = x_2(3x_1 - x_4)x_1$.

5 Discussion

In a forthcoming paper we will generalize parts of the results to rings of arbitrary projective dimension.

References

- [1] J. Abbott, A. Bigatti, M. Kreuzer and L. Robbiano, Computing ideals of points, J. Symb. Comput. 30, 2000, pp. 341-356.
- [2] M. F. Atiyah, I. G. Macdonald. Introduction to commutative algebra. Addison-Wesley Publishing Co., Reading, Mass., 1969.
- [3] B. Buchberger and M. Möller, The construction of multivariate polynomials with preassigned zeroes, Computer Algebra: EUROCAM '82 (J. Calmet, ed.), Lecture Notes in Computer Science 144, 1982, pp. 24-31.
- [4] D. Coppersmith, S. Winograd, Matrix multiplication via arithmetic progressions, J. Symb. Comput. 9, 1990, pp. 251-280.
- [5] R.M. Corless, Editor's Corner: Gröbner bases and Matrix Eigenproblems. SIGSAM Bull. 30, nr 4, 1996, pp. 26-32.
- [6] R.M. Corless, P.M. Gianni, B.M. Trager, A reordered Schur factorization method for zero-dimensional polynomial systems with multiple roots, ISSAC '97: Proceedings of the 1997 international symposium on Symbolic and algebraic computation, 1997.
- [7] J.C. Faugère, P. Gianni, D. Lazard and T. Mora, Efficient Computation of Zero-Dimensional Gröbner Basis by Change of Ordering. J. Symb. Comput. 16, 1993, pp. 329-344.

- [8] A.V. Geramita, P. Maroscia, L. Roberts, Hilbert Function of a Reduced k -algebra, *J. London Math. Soc.*, (2), 28, 1983, pp. 443-452.
- [9] G. Gotzmann, Eine Bedingung für die Flachheit und das Hilbertpolynom eines graduierten Ringes, *Math. Z.* 158, 1978, pp. 61-70.
- [10] W. Gröbner, *Algebraische Geometrie*, Vol 2, Bibliographisches Institut Mannheim (1967-1968).
- [11] S. Lundqvist, Complexity of comparing monomials and two improvements of the Buchberger-Möller algorithm, *Proceedings of MMISC 2008* (J. Calmet, W. Geiselmann and J. Müller-Quade ed.), *Lecture Notes in Computer Science* 5393, 2008, pp. 105-125.
- [12] S. Lundqvist, Vector space bases associated to vanishing ideals of points, 2008, arXiv:0808.3591. Submitted to *Journal of Pure and Applied Algebra*.
- [13] S. Lundqvist, Non-vansihing forms in projective space, in preparation.
- [14] M. G. Marinari, H.M. Möller, and T. Mora, Gröbner bases of ideals defined by functionals with an application to ideals of projective points. *Applicable Algebra in Engineering, Communication and Computing* 4, 1993, pp. 103-145.
- [15] M. G. Marinari, H.M. Möller, and T. Mora, On multiplicities in polynomial system solving. *Trans. Amer. Math. Soc.*, vol 348, 1996, pp. 3283-3321.
- [16] H.M. Möller and H. Stetter, Multivariate polynomial equations with multiple zeros solved by matrix eigenproblems, *Numer. Math.* 70, 1995, pp. 311-329.
- [17] H.M. Möller, R. Tenberg. Multivariate polynomial system solving using intersection of eigenspaces. *J. Symb. Comput.* 30, 2001 pp. 1-19.
- [18] L. Robbiano, Introduction to the theory of Hilbert functions, *Queen's Papers in Pure and Applied Math.*, vol. 85 (1991) B1-B26.
- [19] H. Stetter, *Numerical Polynomial Algebra*, xv+472 pp., Philadelphia: SIAM, 2004.